DEPARTMENT OF SOCIAL SERVICES
INFORMATION SECURITY POLICY

PURPOSE

Promote information security and protect the Department of Social Services' (DSS) information and information processing systems. Ensure the confidentiality, availability, and integrity of data; reduce the risk of data loss by accidental or intentional modification, disclosure, or destruction; and to preserve the department's rights and remedies in the event of such a loss.

SCOPE

This policy applies to:

- all DSS employees, employees of local welfare agencies (LWA), contractors, vendors, volunteers, work experience personnel and other persons and organizations who have a need to use DSS related information or information processing systems,

- all information and information processing systems associated with the Department of Social Services,

- all information and information processing systems associated with other organizations which the Department of Social Services uses.

POLICY STATEMENTS

DSS related information is only to be made known to and utilized by authorized individuals for authorized DSS purposes.

Electronic data processing equipment and programs developed and/or purchased by/for the Department of Social Services are the property of the Department of Social Services and may only be used for authorized purposes.

All DSS related information, data processing equipment, software and data files must be protected from accidents, misuse and unauthorized alteration. Software and data files must be documented and backed up.

Violations of this policy must be reported to the appropriate division/office/agency director and the Division of Information System's (DIS) Information Security Unit. Violations of state and local laws will be reported to the appropriate law enforcement authorities. In the case of lost or missing computer equipment or software, notification must also be made to the Office of Internal Audit.

OBJECTIVES

- Ensure the integrity and protection of information and information processing systems.
- Provide for privacy of privileged or sensitive information.
- Protect information and information processing systems from the hazards of fire, water, misappropriation, misapplication, vandalism or other peril.
- Ensure the department's ability to provide services and benefits to its customers.
- Describe user responsibilities for information security.

REFERENCES

- COV ITRM Policy 90-1 (rev. 5/19/95), Information Technology Security
- COV ITRM Policy 91-1 (1/1/92), Information Systems Development and Maintenance
- COV ITRM Standard 95-1(rev. 1/31/95), Information Technology Security
- COV ITRM Guideline 91-3 (1/1/92), Model Standards for Large-Scope Projects
- COV ITRM Guideline 91-4 (1/1/92), Model Standards for Small-Scope Projects
- COV ITRM Guideline 91-5 (1/1/92), Model Standards for Maintenance and Enhancement Projects
- TANIF Manual 103.1 (1/20/97), :Purpose of Safeguarding of Information and Scope of Regulations
- VDSS/DCSE Manual, Chapter 2 (11/1/96), Confidentiality/Information Release
- USDA/FNS 7 CFR .72.1(c), 272.1(d), Disclosure of Information
- HHS 45 CFR 303.21 and 45 CFR 303.105
- IRS Revenue Procedure Section 6103 (L)(7)(b), Disclosure of Information to Federal, State, and Local Agencies
- Public Law 100-235, Computer Security Act of 1987
- Virginia Social Service Laws 63.1-53 (1996 amended)
- Virginia State Library and Archives, Records Retention and Disposition Schedules (RM-2) (7/94)

RESPONSIBILITIES

Each Person

Each person who use DSS related information must comply with this Information Security Policy. Each person is required to read, sign and abide by the Information Security Access Employee and Consultant Agreement (ISAECA) Form. (Attachment A and B). Each person who uses DSS related information or information processing system is responsible for reporting violations or suspected violations of the Information Security Policy to their division, office, district, region or agency director or designee and the DSS Information Security Administrator.

Any employee who violates the Information Security Policy may be subject to a Standards of Conduct. Violations of the Information Security Policy by others may result in actions which Executive Management deems appropriate under the circumstances.

Executive Management

The Commissioner, through the Information Security Unit, is responsible for assuring that Information Security Policies and Guidelines are developed and distributed to all DSS employees, LWAs, contractors, vendors and other persons and organizations who have a need to use DSS related information and information processing systems. The Commissioner, DSS is responsible for final interpretation of this policy.

Division/Office/District/Regional Management

Division, Office, District and Regional directors are responsible for appointing security officers and backup security officers; developing, implementing, and enforcing procedures within their units which ensure compliance with the Information Security Policies and Guidelines. Directors are also responsible for reporting violations or suspected violations of the Information Security Policy to the DSS Information Security Unit.

Local Agencies

Local agency directors are responsible for appointing security officers and backup security officers; developing, implementing, and enforcing procedures within their agencies which ensures compliance with the Information Security Policies and Guidelines. Local agency directors are responsible for reporting violations or suspected violations of the Information Security Policy to the DSS Information Security Unit.

Security Officers

Division, Office, District, Regional and Local Agency security officers are responsible for assisting employees in obtaining access to information processing resources as needed to allow authorized employees to accomplish their normal daily functions.

DSS Information Security Unit

This unit is responsible for providing technical information, security assistance, and for fostering and overseeing the department's information security program. The unit promotes information security awareness; maintains and distributes Information Security Policies and Guidelines; provides technical assistance to divisions, offices, districts, regions and local agencies in developing, implementing and administering their security programs and procedures; performs risk analysis; investigates alleged security breaches; develops, maintains and disseminates a recovery plan for the department; and trainsinformation systems users on proper methods of securing and controlling those resources.

This Information Security Policy becomes effective on October 1, 1997 and will remain in effect until it is superseded or rescinded by the Commissioner, Virginia Department of Social Services.

Clarence H. Carter, Commissioner

SECURITY POLICIES, REQUIREMENTS AND GUIDELINES

1. SECURITY ADMINISTRATION

BACKGROUND: For an information security policy to be effective, someone in each division, office, region, district and local agency should be assigned the responsibility for developing security procedures and administering the security program in their unit. The individual selected should be cognizant of data processing and information security fundamentals and possess sufficient abilities to develop, implement and enforce information security procedures.

POLICY: Each division, office, region, district and local agency must have an effective security administration function in place.

REQUIREMENTS: Each division, office, district, region and local agency must designate a security officer and backup security officer whose responsibility is to ensure compliance with the DSS Information Security Policies and Guidelines.

Each division, office, district, region and local agency must develop, implement and maintain local information security procedures which effectively implement the DSS Information Security Policies Requirements and Guidelines and ensure their compliance.

Each division, office, district, region and local agency should ensure all of their users of information and information systems are made aware of and receive continuing training on security requirements.

2. CONTINGENCY MANAGEMENT

BACKGROUND: The Council on Information Management (CIM) issued COV ITRM Standard 95-1 which became effective on January 31,1995 requires all state agencies to have a Contingency Management Plan in place.

POLICY: Each division, office, district, region and local agency is responsible for developing, implementing, and testing a contingency management plan which ensures resumption of critical activities in the event of a business disruption.

REQUIREMENTS: The contingency management plan should identify the following:

- The individual(s) responsible for the detailed analysis, planning, documentation and maintenance of the plan.

- Documentation of each unit’s mission, including the organizational, managerial, and technical environment within which an effective Contingency Management Plan must operate.

- Assessment of the risk associated with the most probable types of contingencies and identification of cost effective protective measures to be implemented.

- Assessment of the resources required to implement the contingency management plan.

- Identification, evaluation, and cost benefit analysis of alternative recovery strategies.

- Selection of the alternative that best responds to the contingency management requirements.

- Determine recovery procedures and time frames for execution.

- The Contingency Management Plan should be tested and adjusted where necessary. A copy of the plan should be stored at a remote site.

3. AUTHORIZING ACCESS TO INFORMATION AND INFORMATION PROCESSING SYSTEMS

BACKGROUND: Authority to access information and information processing systems must be evidenced. Properly completed and approved computer system access request forms serve as evidence that the user has the authority to access specific information and information processing systems.

POLICY: Management is responsible for authorizing individuals they supervise the authority to access information and information processing systems.

REQUIREMENTS: Directors, manager and supervisors who are authorized to grant access in information and information processing systems must be identified to the unit's security officer.

The Computer System Access Request (Attachment A) must be completed and retained by the unit's security officer for each person requesting access to DSS Information Systems. If an individual's access needs to be change, new forms must be completed. Local Agencies may use their own forms provided they evidence similar user, system and approval information. (Refer to the Information Security Officer's Manual for procedures for granting access to DSS Information Processing Systems.)

Either the Information Security Employee and Consultant Agreement (Attachment B) or the Information Security Volunteer and Supervisor Agreement (Attachment C) must be completed for all users of DSS related information or information processing systems.

4. PHYSICAL SECURITY - INFORMATION

BACKGROUND: DSS related information is regarded as an asset by the department. As such, it is to be afforded a level of control and protection commensurate with its value and sensitivity to the customer, department, division, office, agency and user.

POLICY: DSS related information is only to be made known to and used by authorized individuals for authorized purposes and must be protected against unauthorized use, theft, vandalism, or other peril.

REQUIREMENTS: All information, regardless of the medium, that contains client specific information is considered confidential and must be restricted to personnel who are authorized to use the information.

Use/disclosure of client, financial and statistical information shall only be made by individuals who have the authority to do so.

Information provided by internal or external sources can only be made available to personnel who have been identified by the owner of the data as having a need to know.

Confidential information must be protected from unauthorized access at all times.

Confidential information should be properly disposed of when it has reached its retention date or when the owner of the data determines it is no longer needed. The retention of financial, statistical and client information must comply with the Virginia State Library and Archives, Record Retention and Disposition Schedule (RM-2).

5. PHYSICAL SECURITY - INFORMATION PROCESSING SYSTEMS AND EQUIPMENT

BACKGROUND: Information processing systems and equipment are department assets and must be afforded a level of security commensurate with their value and their ability to access information which is important to the customer, department, division, office, agency, or user.

POLICY: Information processing systems and equipment must be protected against unauthorized use, theft, vandalism, fire/smoke/water damage, misappropriation, misapplication, or other peril.

REQUIREMENTS: Only authorized personnel users should be permitted to use information processing systems and equipment.

Computer equipment and programs should be located in areas which afford protection from disasters.

Computer equipment and programs must be inventoried biannually.

GUIDELINES: Computer equipment, software and documentation should be located in areas that have restricted access and can be monitored.

Portable computer equipment (i.e. laptop and notebook computers) should be locked up when not in use or cabled to the desk/work station.

6. PASSWORDS

BACKGROUND: An effectively implemented passwords control system can limit access to information systems to authorized personnel. To be effective, the passwords should be changed frequently, they should not be shared or disclosed to others and they should not be easily guessed.

POLICY: Individual password must be used to control access to information processing systems.

GUIDELINES: Each individual granted authority to access information processing systems should be assigned a unique logon ID which will require a password for access.

The password should be a series of characters/numbers that is only meaningful to the individual.

Password should not be the names of family members, pets, friends or associates.

Passwords should not be a series of repeating or sequential characters or numbers nor should they be Social Security or telephone numbers.

Passwords should be changed monthly.

Passwords should not be written or stored in a manner accessible to others.

Each individual is responsible for ensuring their password is kept confidential and immediately reporting suspected compromise or unauthorized use to their security officer.

7. BACKING UP INFORMATION

BACKGROUND: Disasters happen and they don't have to be in the category of fires, floods and tornados to cause a major disruption in our ability to get the job done. The accidental loss of information on personal computer and floppy disks is far more common than natural disasters. An effective backup system is one of the best ways of assuring the ability to recover after a disaster.

POLICY: Electronic information (data files) that is a part of a benefit, service delivery or financial management system should be periodically backed up and stored off site at least weekly. Mainframe data and user data stored on the LAN is backed up and stored off site daily.

GUIDELINES: The more important information is to a priority function, the more frequently it should be backed up.

Information that would be costly, time consuming or impossible to reconstruct should be backed up frequently.

A backup copy of important information should be routinely rotated off site. Off site locations should be determined by the user or his/her supervisor.

Backups should be retained until a newer backup renders the older backup obsolete.

8. ILLEGAL COPYING

BACKGROUND: The unauthorized duplication of software, manuals and other materials is theft. These products reflect a substantial investment of time, talent and money by the developers. Unauthorized duplication deprives the developers of fair compensation.

POLICY: The duplication of software, manuals, or other materials in violation of copyright laws and vendor licensing agreements is strictly forbidden. Infractions of this policy may result in a

Standards Of Conduct being issued as well as civil and criminal penalties.

REQUIREMENT: Violations of this policy must be reported to the appropriate division, office, or agency director and to the Division of Information System's Information Security Unit. Violations of state and local laws will be reported to the appropriate law enforcement authorities.

9. USING PERSONAL SOFTWARE ON DSS COMPUTERS

BACKGROUND: The Department of Social Services discourages the use of personal software on state owned computer; however, the department realizes that there may be a need for limited use of personal software (non-departmental software) for the efficient operation of certain functions. There are two primary concerns which this policy addresses:

- Personal software may only be used in accordance with copyright laws and license agreements.

- Personal software must not be used to produce critical department data and reports. Such use may lead to extra work for others should the personal software stop working, be removed from the PC or the individual knowledgeable in its use be unavailable. If a software package is needed to perform a required task, submit a purchase request for the product.

POLICY: The Department of Social Services allows the use of personally owned software on DSS personal computers providing the software is:

- Used in accordance with copyright laws and the licensing agreement of the company that produced the software;

- Required to perform DSS business related activities; and

- Approved for use in writing by the user's division director designated representative.

This policy applies to commercially produced software, shareware, public domain software and freeware.

The installation of personal software onto the Department's Network is strictly forbidden unless authorized in writing by the Manager of the NetCentric Unit.

Violations of this policy will be dealt with through the Standards of Conduct.

REQUIREMENTS: If the software license allows the use of the personally acquired software on a home computer and an office computer, it may be used on DSS computers if the director approves.

If the software license allows the use of the software on one computer only, then it may not be installed on more than one computer at a time.

Users must have in their possession the original diskettes and software documentation provided by the vendor.

The “Request To Use Personal Software on Department Computers” form (Attachment C) must be completed to evidence management approval and retained by the unit’s security officer.

10. ANTI-VIRUS SOFTWARE

BACKGROUND: The availability of departmental data is paramount to the successful completion of the DSS mission. PC viruses are proliferating at a staggering rate and the potential for infection increases daily. We must ensure that department information processing systems remain virus free at all times.

POLICY: Anti-virus software must be installed and must be operational on all personal computers and servers that access DSS information or information processing system.

REQUIREMENTS: All personal computers and servers that access DSS information or information processing systems must have the department’s standard anti-virus software installed and it must be operational.

11. INFORMATION SYSTEMS - DEVELOPMENT AND CHANGE CONTROL

MAINFRAME SYSTEMS

BACKGROUND: DSS' information systems serve to support the department's mission. It is imperative that any changes made to these systems be authorized and be performed in a controlled manner.

POLICY: Information system development and maintenance projects must implement a methodology that is based on structure and discipline and that meets the COV ITRM Guidelines 91-3 (Model Standards for Large Scope Projects), 91-4 (Model Standards for Small Scope Projects) and 91-5 (Model Standards for Maintenance and Enhancement Projects).

REQUIREMENTS: DSS System Development Methodology (SDM) must be formalized and documented to provide uniform guidance to systems and programming staff on system development and maintenance activities.

Initiation and approval of system development and maintenance projects will follow COV ITRM Guidelines (91-3, 91-4 and 91-5).

Development and maintenance projects must be supported by the DSS System Development Life Cycle; generating appropriate deliverable for each phase and obtaining appropriate management approval before continuing on to the next phase.

Development and maintenance projects must have approved work plans with appropriately detailed tasks and timetables.

Only properly tested, documented and approved systems and modifications will be implemented.

If problem resolution requires program changes to be implemented immediately, these requirements should be applied retroactively to the program changes on the next business day.

The Office of Internal Audit should be kept apprised of all system development activities.

PERSONAL COMPUTER BASED SYSTEMS

BACKGROUND: More and more people are learning how to use PCS and discovering techniques to help them perform their every-day tasks more efficiently and effectively. Information is being down-loaded from mainframe computers to PCS and users of this information are developing spreadsheet and data base applications which manipulate the information for various needed purposes. The department encourages its employees to be creative and seek better ways to satisfy their information needs. There are however, documentation, testing and approval requirements that must be observed when an information user develops applications (spreadsheets, data bases, fourth generation languages, MAPPER, query language processors, report writers, etc.) that use customer information or produce information used in decision making or financial/statistical reporting.

POLICY: PC systems using customer information or producing information used in decision making or financial/statistical reporting must be documented, tested and approved.

REQUIREMENTS: Required documentation includes a description of the application to include its: author, purpose, inputs, outputs, processes, calculations, controls, security, interfaces with other systems/processes, execution instructions, run schedule, error/exception handling, intended user and information retention.

Documentation must be of sufficient detail to provide someone other than the developer enough information to maintain and run the application.

The accuracy of the application as to outputs, processes, calculations, controls, security, execution instructions, run schedule, and error/exception handling must be verified in writing by someone other than the developer.

Responsible management must review and approve the application prior to implementation.

12. NETWORKS

BACKGROUND: The department sponsors an Intranet, known as Network 2000, which connects the central, regional and district offices and local agencies together. This Intranet is the primary vehicle through which department information and system resources are shared.

POLICY: Adequate controls ensuring the security and integrity of the networks which access DSS related information and information systems must be implemented and functioning.

REQUIREMENTS: A department network administrator and backup administrator, whose primary responsibility is to coordinate and manage network activities must be appointed.

All software programs must be approved by the network administrator before being loaded into any of the department's file servers. Program files (e.g. .exe, .dll, .bat, and any other executable files) are not to be written to any network drives unless authorized in writing by the network administrator.

All programs and data must be scanned by the department's anti-virus software before being introduced into the network.

File servers shall be backed up on a frequency sufficient to permit timely recovery and minimal disruption. Weekly, full backups must be performed for each file server. On a daily basis, incremental backups should be performed.

All backups must be stored off-site to ensure safety of the media.

13. INTERNET

BACKGROUND: Department staff are encouraged to use the Internet to further DSS's mission; provide effective services of the highest quality to our customers; discover innovative and creative ways to use resources and improve our services and promote staff development. However, users need to remember that:

Technical attacks will be made against DSS Information systems.

Internet access opens an information conduit by which sensitive, and potentially private, information could be released onto the open network and the world.

The Internet is not a secure environment and users should assume that whatever they are doing is being monitored both internally as well as by individuals interested in compromising DSS.

User activities are traceable to the Commonwealth of Virginia, DSS, and the user.

POLICY: This policy applies to department employees, contractors and volunteers (department staff). If local agency management allows their staff access to the Internet, this policy and the requirements below will minimally apply to local agency users (agency staff).

- Department and agency staff (users) may use the Internet for direct job-related purposes, professional contacts and career development activities. Incidental personal use is tolerated; however, extensive or recurring personal use is forbidden.

- Users are allowed full E-mail capabilities and are permitted to participate in various forums.

- For security and releasability reasons information pertaining to the department, its clients, and others who do business with the department may not be release out to the Internet unless it is encrypted using department-sponsored encryption software.

- Users are responsible for reading and complying with the Code of Virginia, Chapter 52

(Attachment E).

Forbidden acts:

- Use of facilities and/or services for illegal, wrongful or commercial purposes.

- Visiting sites which are restricted by the Code of Virginia, Chapter 52.
- The willful introduction of computer viruses or other disruptive/destructive programs into the department's network or into external networks.

- Intentional attempts to "crash" network systems or programs.

- Use of system and/or networks in attempts to gain unauthorized access.

- Use of system and/or networks for purposes of snooping, probing, or otherwise connecting to a node or nodes in a manner which is deemed not to be of an authorized nature.

- Decrypting system or user passwords.

- Downloading files without department-sponsored anti virus software being actively running.

- Uploading, downloading, modifying or removing files on any node in the network for which such action is not authorized.

REQUIREMENTS: Users must be authorized to use the Internet, comply with all stated policies and will be held accountable for their activities.

14. ELECTRONIC MAIL (E-MAIL)

BACKGROUND: Department and local agency staff are encouraged to use E-mail for transmitting department related business messages. E-mail that is transmitted over the department's Intranet is done so on dedicated lines; therefore, these transmissions are relatively secure because they do not go through any non-department servers. E-mail sent over the Internet however, is not secure because the number and location of servers which handle E-mail traffic are unknown and out of the department's control.

POLICY: All information pertaining to the department, its clients, and others who do business with the department, that is transmitted via E-mail, must be sent by a secure means.

REQUIREMENTS: Only department-sponsored E-mail systems and networks (Network 2000) may be used to transmit information pertaining to the department, its clients and others who do business with the department.

Only authorized individuals may send information pertaining to the department, its clients and others who do business with the department over the Internet.

Any information pertaining to the department, its clients and others who do business with the department which is released out to the Internet must be encrypted using department-sponsored encryption software.

The policies and requirements stipulated in 4. Physical Security - Information and 13. Internet applies to E-mail.

15. COMPUTER GAMES

BACKGROUND: In memos from the Governor’s Office and the Secretary of Health and Human Services, playing computer games on state-owned computers and/or on state time shall not be done.

POLICY: Computer games will not be loaded or played on state-owned computers. Computer games are not to be played on state-time.

REQUIREMENTS: Same as Policy. Violations of this policy will be dealt with as a Group II Offence under the Standards of Conduct.

SECURITY POLICY DICTIONARY

Access - The ability to view, change or communicate with a computer system. Access includes execution of programs, reading and writing to files and deleting files or data.

ADP - Automated Data Processing

Authorized individual - Person granted the ability to access department information.

Backup - The copying of information to a medium from which it can be restored if the original is destroyed or damaged. Full backups copy all data in the system. Incremental backups copy only the information that has been changed since the last full backup.

Confidentiality - Ensuring that information is disclosed to authorized individuals only.

Contingency Management - Administration of a plan for responding to emergency situations. The plan includes performing backups., preparing critical facilities that can ensure continuity of operations in the event of an emergency. It is synonymous with disaster recovery plan.

Customer - Person requesting benefits and or services from the department.

E-mail or Electronic mail - Personal communications consisting of memos, letters, files, voice or video sent over computer networks. When public networks (e.g. The Internet) are used the sender has no control over message routing; therefore, Internet traffic is not secure. When private networks are used (e.g. DSSP, GroupWise, and DSS's soon to be implemented Wide Area Network) the traffic is secure.

Guidelines - Statements or rules created to allow the development or local procedures to comply with this security policy.

Integrity - Ensuring information is changed only in a specified manner. Maintaining information in what is considered to be an accurate and correct format.

Internet - A loose confederation of autonomous networks distributed among military, academic, private and corporate sites that are interconnected via an open communications protocol known as TCP/IP. The Internet is a interconnected group of individual computers and networks around the world.

Intranet - Networks which utilize World-Wide Web technologies but which are limited to a single company or organization. Intranets are used to distribute information within an organization using resources developed for the Internet, but without to security concerns associated with Internet connectivity.

ISAECA - Information Security Access Employee and Consultant Agreement. A notarized agreement between the Department of Social Services and anyone who has access to DSS information or information processing systems, to maintain the confidentiality of DSS (and other agencies) information and to only use this information or system for authorized purposes.

LWA - Local Welfare Agency.

Network 2000 - The name of the Department of Social Services' Intranet. This network connects users in central, district and regional offices and local agencies together. This is a secure network. Messages transmitted through Network 2000 cannot be intercepted or attacked by individuals who are not permitted on the network.

Personal Software - Software not provided by the department, division, office or local agency.

Physical Security - Protection of computer systems and related buildings and equipment form fire, natural disaster, environmental hazards and intrusion. The use of locks, keys, and administrative measures to control access to computer systems and facilities.

Policy - A high-level plan identifying the department's philosophy regarding its information and information processing systems.

Public Domain Software - Software that is available free of charge to anyone. Registration is usually not required.

Requirements - Actions that must be included in the security procedures.

Resources - Items having operational, monetary or material value owned, leased or under care and custody of the department.

Sensitive Information - Information that, if lost or compromised would negatively effect the ability of the department to provide services and benefits to its customers (e.g. confidential information about recipients of DSS benefits or services). Also known as privileged

Shareware. Software which may be copied and provided to anyone for evaluation purposes only. If the shareware is to be used, it must be must be registered and a fee paid to the developer in accordance with the licensing agreement.

Risk - The vulnerability of a particular threat to exploit an information resource's availability.

World-Wide Web (WWW) - A network of servers that uses hypertext links to find and access files on the Internet. Web browsers (e.g. Telnet, Gopher, etc.) allow you to view documents on servers around the world without having to know where the information is stored.

VIRGINIA DEPARTMENT OF SOCIAL SERVICES
COMPUTER SYSTEM ACCESS REQUEST

This form must be completed by the Unit's Security Coordinator and forwarded to the Virginia Department of Social Services, Information Security Office for anyone requiring access to DSS information systems.

TODAY'S DATE: ___/___/___ EFFECTIVE DATE: ___/___/___ (provide 1 weeks lead time)

Γ ADD Γ CHANGE* Γ DELETE* Γ Classified Γ P-14 ΓVolunteer Γ Contractor**
* LOGON ID(s)________________________________

USER'S FULL NAME: ________________________________ SSN: ________________________

TITLE/POSITION:_____________________________________ PHONE:______________________

DIVISION/OFFICE:____________________________________UNIT:_______________________

USER'S GROUP(S):_________________________________ (for sharing data with others in group(s))

ACCESS REQUIRED - To be completed by user's supervisor (check all that are required):

Γ LAN Γ REMOTE DIAL IN Γ INTERNET
Γ UNISYS (TIP) build user's logon ID like ______________________or specify applications
required_______________________________________ FIPS No:_____ VACIS No._____

Γ APECS (complete and attach APECS System Access Request Form)

Γ IMS Γ VEC Γ DMV Γ TAX Γ SVES

Γ DMAS (complete and attach DMAS MMIS Security Access Request Form)

Γ SSAMS (build user's logon ID like)__________________

Γ CARS (build user's logon ID like)___________________

Other system access required____

User Signature / Date:____

Supervisor Signature / Date:____

Unit Security Coordinator / Date:______________________________** Retains contractor's ISECA Form

SSAMS Security Administrator / Date:_________________________________

LAN Administrator / Date:____

DSS Information Security Officer / Date:_______________________________

RETURN COMPLETED FORM TO THE DSS INFORMATION SECURITY OFFICE

DSS Access Request Form - ACCESREQ (9/97) *Attachment A*

COMMONWEALTH OF VIRGINIA
DEPARTMENT OF SOCIAL SERVICES

Information Security Employee and Consultant Agreement

I understand that Department of Social Service (DSS) related information is only to be made known to and utilized by authorized individuals for authorized DSS purposes.

I understand that data processing equipment and application programs developed by or purchased by/for DSS are the property of DSS and may only be used for authorized purposes.

I understand that all DSS related information, data processing and telecommunications equipment, networks, software and data files must be protected from accidents, misuse, and unauthorized disclosure.

I understand that passwords and file protection keys are confidential and are not to be revealed to anyone who does not require them in the normal performance of their duties.

I agree not to create, execute or place into production any unauthorized programs, runs or transactions. I further agree not to view or update any DSS related information outside my specific area of responsibility.

By signing this agreement, I hereby certify that I have read and understand the DSS Information Security Policy and the statements above and agree to abide by them. I understand that ANY violations of the DSS Information Security Policy or the statements above may result in my receiving a Group II or Group III Standards of Conduct Offense; and prosecuting action may be undertaken if I knowingly and intentionally use any DSS related information, information processing systems or equipment for fraudulent, extorsive or destructive purposes. Furthermore, I understand it is my responsibility to report any DSS Information Security violations or suspected violations to DSS management and/or security staff.

Executed this ______ day of ______________, 19___ at ________________________________
Division / Office / Locality / Agency

______________________________________ ______________________________________
Print Employee / Consultant Name Signature

This instrument was acknowledged before me this ______ day of ______________, 19_____

by __________________________________ ______________________________________
Print Witness Name Signature

DSS Security Form - ISECA (9/97) *Attachment B*

COMMONWEALTH OF VIRGINIA
DEPARTMENT OF SOCIAL SERVICES

Information Security Volunteer and Supervisor Agreement

VOLUNTEER:

I understand that Department of Social Service (DSS) related information is only to be made known to and utilized by authorized individuals for authorized DSS purposes.

I understand that data processing equipment and application programs developed by or purchased by/for DSS are the property of DSS and may only be used for authorized purposes.

I understand that all DSS related information, data processing and telecommunications equipment, networks, software and data files must be protected from accidents, misuse, and unauthorized disclosure.

I understand that passwords and file protection keys are confidential and are not to be revealed to anyone who does not require them in the normal performance of their duties.

I agree not to create, execute or place into production any unauthorized programs, runs or transactions. I further agree not to view or update any DSS related information outside my specific area of responsibility.

SUPERVISOR:

I agree to provide competent, intensive supervision of the volunteer worker. I agree to request the minimum access level required for the volunteer to be productive.

I agree to report to the security staff when the volunteer worker no longer requires access or is no longer volunteering with DSS, this includes unknown absences of one week.

By signing this agreement, I hereby certify that I have read and understand the DSS Information Security Policy and the statements above and agree to abide by them. I understand that ANY violations of the DSS Information Security Policy or the statements above may result in disciplinary action, which can include dismissal from my volunteer duties; and prosecuting action may be undertaken if I knowingly and intentionally use any information obtained by me at DSS for fraudulent, extorsive or destructive purposes. Furthermore, I understand it is my responsibility to report any DSS Information Security violations or suspected violations to DSS management and /or security.

Executed this ______ day of ______________, 19___ at ________________________________
Division / Office / Locality / Agency

______________________________________ ______________________________________
Volunteer's Name Supervisor's Name

DSS Security Form - ISECAVOL (9/97) *Attachment C*

DEPARTMENT OF SOCIAL SERVICES
REQUEST TO USE PERSONAL SOFTWARE ON DEPARTMENT COMPUTERS

POLICY SUMMARY: The Department of Social Services recognizes the need for the limited use of personal software (non-departmental software) for efficient operation of certain functions. The Department allows the use of personally owned software on DSS personal computer providing the software is:

- Used in accordance with copyright laws and the licensing agreement of the company that produced the software;

- Required to perform DSS business related activities; and

- Approved for use in writing by the division director or designated representative.

This policy applies to commercially produced software, shareware, public domain software and freeware. The use of personal software in information processing systems connected to the Department's Network is strictly forbidden unless authorized in writing by the Manager of the NetCentric Unit.

Violations of this policy will be dealt with through the Standards of Conduct.

General Information:

1. User Name:___________________________

2. Division/office/region/district/agency:_______________________ Unit ________________

3. Property Tag No.:______________ Location:______________________________________

4. Application Program Name:____

5. Date Installed:____________

6. Reason Software is Required:____

____

I acknowledge that I have read and understand the Policy Summary above and that this request is in compliance with the Department of Social Services' Policy related to the use of personal software.

Requestor Signature/Date:____________________________________

Approver Signature/Date:_____________________________________

DSS Security Form - PERSOFT (9/97) *Attachment D*

CHAPTER 52.

RESTRICTIONS ON STATE EMPLOYEE ACCESS TO INFORMATION INFRASTRUCTURE.

§ **2.1-804. Definitions.**—For the purpose of this chapter:

"Agency" means any agency, authority, board, department, division, commission, institution, institution of higher education, bureau, or like governmental entity of the Commonwealth, except the Department of State Police.

"Information infrastructure" means telecommunications, cable, and computer networks and includes the Internet, the World Wide Web, Usenet, bulletin board systems, on-line systems, and telephone networks.

"Sexually explicit content" means (i) any description of or (ii) any picture, photograph, drawing, motion picture film, digital image or similar visual representation depicting sexual bestiality, a lewd exhibition of nudity, as nudity is defined in § 18.2-390, sexual excitement, sexual conduct or sadomasochistic abuse, as also defined in § 18.2-390, coprophilia, urophilia, or fetishism. (1996, c. 382.)

§ **2.1-805. Restriction on agency employee access via computers to materials with sexually explicit content.**—Except to the extent required in conjunction with a bona fide, agency-approved research project or other agency-approved undertaking, no agency employee shall utilize agency-owned or agency-leased computer equipment to access, download, print or store any information infrastructure files or services having sexually explicit content. Such agency approvals shall be given in writing by agency heads, and any such approvals shall be available to the public under the provisions of the Virginia Freedom of Information Act (§ 2.1-340 et seq.) of Title 2.1. (1996, c. 382.)

§ **2.1-806. Agencies to inform employees of chapter's provisions.**—
All agencies shall immediately furnish their current employees copies of this chapter's provisions, and shall furnish all new employees copies of this chapter concurrent with authorizing them to use agency computers. (1996, c. 382.)